(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－6232

(43)公開日　平成9年(1997)1月10日

(51)Int.Cl.[6]		識別記号	庁内整理番号	FI			技術表示箇所
G09C	1/00		7259－5J	G09C	1/00		
G06F	9/06	550		G06F	9/06	550A	
H04L	9/00			H04L	9/00	Z	
	9/10						
	9/12						

審査請求　未請求　請求項の数21　ＯＬ　（全 20 頁）

(21)出願番号　特願平7－154513

(22)出願日　平成7年(1995)6月21日

(71)出願人　000006932
リコーエレメックス株式会社
名古屋市中区錦二丁目2番13号

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込1丁目3番6号

(72)発明者　坂　康彦
愛知県名古屋市東区泉2丁目28番24号　リコーエレメックス株式会社内

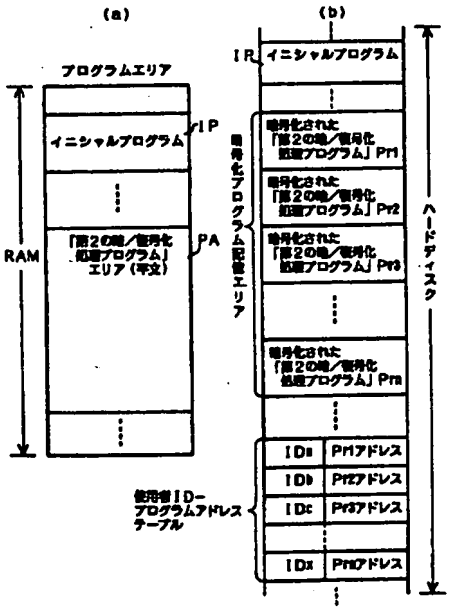
(74)代理人　弁理士　足立　勉

(54)【発明の名称】　暗号化システム、復号化システム、情報秘匿処理システムおよび情報秘匿通信システム

(57)【要約】

【目的】　プログラムが改竄されることなく暗号化・復号化を効率的に行うことができるシステムを提供すること。

【構成】　イニシャルプログラムIPにより、パスワードが合致すると情報処理装置からICカードへ暗号化された暗／復号化処理プログラムPr1,Pr2,…が送信され、ICカードはこのプログラムを正当使用者の復号化鍵にて復号化し送り返す。情報処理装置はこのプログラムを作業メモリ領域PAに配置して起動しデータの暗／復号化処理を行う。従って通常、プログラムは暗号化されているので第三者により解析されず改竄もできない。正当使用者がデータの処理を完了した後はその平文のプログラムは消去されるため、処理後も平文のプログラムは残っていず、プログラムの安全性が確保される。このため暗号化／復号化処理毎にプログラムの記憶媒体を保管場所から取り出して情報処理装置にセットする作業をしなくても良く効率的に暗号化作業ができる。



1

【特許請求の範囲】

【請求項1】プログラムに基づく暗号化処理によりデータを暗号化する暗号化システムにおいて、

前記プログラムを、使用者に対応する第1暗号化鍵により暗号化した状態で記憶するプログラム暗号化記憶手段と、

前記プログラム暗号化記憶手段内から、使用者に対応する第1暗号化鍵にて暗号化された前記プログラムを読み出すプログラム読出手段と、

前記プログラム読出手段により読み出された前記プログラムを、使用者に対応する復号化鍵により復号化するプログラム復号化手段と、

前記プログラム復号化手段により復号化されたプログラムを起動させることにより、暗号化対象データを第2暗号化鍵にて暗号化させて暗号化データとするプログラム起動手段と、

前記プログラム起動手段にて暗号化対象データの暗号化が完了すると、復号されて起動対象となった前記プログラムを消去するプログラム消去手段と、

を備えたことを特徴とする暗号化システム。

【請求項2】更に、

前記第2暗号化鍵を、第3暗号化鍵にて暗号化する鍵暗号化手段と、

前記鍵暗号化手段にて暗号化された前記第2暗号化鍵を、前記暗号化データに付加する鍵付加手段と、

を備えた請求項1記載の暗号化システム。

【請求項3】前記鍵付加手段が、前記プログラムの機能として実現されている請求項2記載の暗号化システム。

【請求項4】前記プログラムが、第2暗号化鍵を演算にて求める請求項1～3のいずれかに記載の暗号化システム。

【請求項5】本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、

前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、

前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段を備える請求項1記載の暗号化システム。

【請求項6】本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、

前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム復号化手段、前記プログラム起動手段、および前記プログラム消去手段を備え、

前記付属装置が、前記第3暗号化鍵を記憶するとともに、前記鍵暗号化手段を備える請求項3記載の暗号化システム。

2

【請求項7】本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、

前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、

前記付属装置が、前記使用者に対応する復号化鍵および前記第3暗号化鍵を記憶するとともに、前記プログラム復号化手段および前記鍵暗号化手段を備える請求項3記載の暗号化システム。

【請求項8】前記付属装置が、前記第3暗号化鍵を、復号化を許可する者の管理コードと対応したリストとして記憶する請求項6または7記載の暗号化システム。

【請求項9】前記付属装置が、前記復号化鍵または前記第3暗号化鍵を直接記憶せず、前記復号化鍵または前記第3暗号化鍵が必要とされた場合に、対応する管理コードを用いた演算にて、前記復号化鍵または前記第3暗号化鍵を生成する請求項5～7のいずれかに記載の暗号化システム。

【請求項10】前記プログラムが、所定時間以内に使用者により次の入力操作が行われない場合に、自己の処理を中止して、前記プログラム消去手段の処理を実行させる機能を有する請求項1～9記載の暗号化システム。

【請求項11】プログラムに基づく復号化処理により暗号化データを復号化する復号化システムにおいて、

前記プログラムを、使用者に対応する第1暗号化鍵により暗号化した状態で記憶するプログラム暗号化記憶手段と、

前記プログラム暗号化記憶手段内から、使用者に対応する第1暗号化鍵にて暗号化された前記プログラムを読み出すプログラム読出手段と、

前記プログラム読出手段により読み出された前記プログラムを、使用者に対応する復号化鍵により復号化するプログラム復号化手段と、

前記プログラム復号化手段により復号化された前記プログラムを起動させることにより、暗号化データを第2復号化鍵にて復号化させて復号化データとするプログラム起動手段と、

前記プログラム起動手段にて暗号化データの復号化が完了すると、復号化されて起動対象となった前記プログラムを消去するプログラム消去手段と、

を備えたことを特徴とする復号化システム。

【請求項12】更に、

前記暗号化データに含まれる暗号化された第2復号化鍵を、使用者に対応する復号化鍵にて復号化する鍵復号化手段を備えた請求項11記載の復号化システム。

【請求項13】本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、

前記本体装置が、前記プログラム暗号化記憶手段、前記

プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、
前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段を備える請求項１１記載の復号化システム。
【請求項１４】本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、
前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム復号化手段、前記プログラム起動手段、および前記プログラム消去手段を備え、
前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記鍵復号化手段を備える請求項１２記載の復号化システム。
【請求項１５】本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、
前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、
前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段および前記鍵復号化手段を備える請求項１２記載の復号化システム。
【請求項１６】前記付属装置が、前記復号化鍵を直接記憶せず、前記復号化鍵が必要とされた場合に、対応する管理コードを用いた演算にて、前記復号化鍵を生成する請求項１３～１５のいずれかに記載の復号化システム。
【請求項１７】前記プログラムが、所定時間以内に使用者により次の入力操作が行われない場合に、自己の処理を中止して、前記プログラム消去手段の処理を実行させる機能を有する請求項１１～１６記載の復号化システム。
【請求項１８】請求項１～１０のいずれか記載の暗号化システムと請求項１１～１７記載の復号化システムとが組合わされてなる情報秘匿処理システム。
【請求項１９】前記暗号化データを通信回線を介して相手方に送信する送信手段を備える請求項１～１０のいずれか記載の暗号化システム。
【請求項２０】前記暗号化データを通信回線を介して受信する受信手段を備える請求項１１～１７のいずれか記載の復号化システム。
【請求項２１】請求項１９記載の暗号化システムと請求項２０記載の復号化システムとが組合わされてなる情報秘匿通信システム。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、プログラムに基づく暗号化処理によりデータを暗号化する暗号化システム、プログラムに基づく復号化処理により暗号化データを復号化する復号化システム、更にこれらの機能を有する情報秘匿処理システムおよび情報秘匿通信システムに関する。
【０００２】
【従来の技術】従来、情報（「データ」とも言う。）内容を秘匿するための手法として、暗号化鍵を用いて秘匿したい情報を暗号化する処理が知られている。情報が一旦暗号化されると、同一の暗号化鍵あるいは特定の復号化鍵を用いないと人間が解読できる状態に戻すことはできないため、そのような暗号化鍵や復号化鍵を有していない他人にとってはその情報の内容を秘密にすることができる。
【０００３】しかし、暗号化鍵や復号化鍵（以下、「暗／復号化鍵」として表す。）が漏洩すれば、たちまち他人に情報が解読されてしまうことから、この暗／復号化鍵に対しても、別の暗号化鍵にて暗号化して保管することにより安全性を高めるファイルセキュリティシステムが提案されている（特開平６－１０２８２２号公報）。
【０００４】
【発明が解決しようとする課題】しかし、このようなシステムにおいても、次のような問題が存在した。すなわち、情報の暗号化処理あるいは情報解読のための復号化処理は、一般的には、コンピュータシステムを用いた情報処理装置にて、暗号化プログラムあるいは復号化プログラム（以下、「暗号化・復号化プログラム」として表す）によりなされるのが普通である。
【０００５】この暗号化・復号化プログラムにより、情報が暗号化され、更に安全性を高めるために、その暗／復号化鍵まで暗号化した場合、一見、その情報自体は極めて安全であるように考えられる。ところが、この暗号化・復号化を行う暗号化・復号化プログラム自体は、情報自体よりも無防備であることが多い。もし、この暗号化・復号化プログラムのアルゴリズムが第三者により解析されると、暗号化された情報の解読に利用される恐れがある。
【０００６】また、第三者が、その暗号化・復号化プログラム自体を、正当な使用者に解らないように改竄し、第三者が知っている暗号化鍵にて暗号化する機能を付加することにより、その後、暗号化された情報をすべて第三者が解読してしまう恐れもある。更に、暗号化・復号化プログラム内に、暗号化する前の平文状態（暗号化されていない状態を言う。）の情報を第三者が管理する領域にもコピーしてしまう機能を付加する恐れもあった。
【０００７】勿論、暗号化・復号化プログラムを使用しない場合には、暗号化・復号化プログラムを厳重に保管することも考えられるが、使用毎に、フロッピー等を保管場所から取り出して、情報処理装置にセットして暗号化・復号化プログラムをロードする処理を行わなくてはならず、暗号化・復号化処理が効率的に行うことができない。

【０００８】本発明は、第三者に改竄されることなく、かつ暗号化・復号化を効率的に行うことができる暗号化システム、復号化システム、情報秘匿処理システムおよび情報秘匿通信システムを提供することを目的とする。

【０００９】

【課題を解決するための手段】請求項１記載の発明は、プログラムに基づく暗号化処理によりデータを暗号化する暗号化システムにおいて、前記プログラムを、使用者に対応する第１暗号化鍵により暗号化した状態で記憶するプログラム暗号化記憶手段と、前記プログラム暗号化記憶手段内から、使用者に対応する第１暗号化鍵にて暗号化された前記プログラムを読み出すプログラム読出手段と、前記プログラム読出手段により読み出された前記プログラムを、使用者に対応する復号化鍵により復号化するプログラム復号化手段と、前記プログラム復号化手段により復号化されたプログラムを起動させることにより、暗号化対象データを第２暗号化鍵にて暗号化させて暗号化データとするプログラム起動手段と、前記プログラム起動手段にて暗号化対象データの暗号化が完了すると、復号されて起動対象となった前記プログラムを消去するプログラム消去手段と、を備えたことを特徴とする暗号化システムである。

【００１０】請求項２記載の発明は、更に、前記第２暗号化鍵を、第３暗号化鍵にて暗号化する鍵暗号化手段と、前記鍵暗号化手段にて暗号化された前記第２暗号化鍵を、前記暗号化データに付加する鍵付加手段と、を備えた請求項１記載の暗号化システムである。

【００１１】請求項３記載の発明は、前記鍵付加手段が、前記プログラムの機能として実現されている請求項２記載の暗号化システムである。請求項４記載の発明は、前記プログラムが、第２暗号化鍵を演算にて求める請求項１～３のいずれかに記載の暗号化システムである。

【００１２】請求項５記載の発明は、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段を備える請求項１記載の暗号化システムである。

【００１３】請求項６記載の発明は、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム復号化手段、前記プログラム起動手段、および前記プログラム消去手段を備え、前記付属装置が、前記第３暗号化鍵を記憶するとともに、前記鍵暗号化手段を備える請求項３記載の暗号化システムである。

【００１４】請求項７記載の発明は、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、前記付属装置が、前記使用者に対応する復号化鍵および前記第３暗号化鍵を記憶するとともに、前記プログラム復号化手段および前記鍵暗号化手段を備える請求項３記載の暗号化システムである。

【００１５】請求項８記載の発明は、前記付属装置が、前記第３暗号化鍵を、復号化を許可する者の管理コードと対応したリストとして記憶する請求項６または７記載の暗号化システムである。請求項９記載の発明は、前記付属装置が、前記復号化鍵または前記第３暗号化鍵を直接記憶せず、前記復号化鍵または前記第３暗号化鍵が必要とされた場合に、対応する管理コードを用いた演算にて、前記復号化鍵または前記第３暗号化鍵を生成する請求項５～７のいずれかに記載の暗号化システムである。

【００１６】請求項１０記載の発明は、前記プログラムが、所定時間以内に使用者により次の入力操作が行われない場合に、自己の処理を中止して、前記プログラム消去手段の処理を実行させる機能を有する請求項１～９記載の暗号化システムである。

【００１７】請求項１１記載の発明は、プログラムに基づく復号化処理により暗号化データを復号化する復号化システムにおいて、前記プログラムを、使用者に対応する第１暗号化鍵により暗号化した状態で記憶するプログラム暗号化記憶手段と、前記プログラム暗号化記憶手段内から、使用者に対応する第１暗号化鍵にて暗号化された前記プログラムを読み出すプログラム読出手段と、前記プログラム読出手段により読み出された前記プログラムを、使用者に対応する復号化鍵により復号化するプログラム復号化手段と、前記プログラム復号化手段により復号化された前記プログラムを起動させることにより、暗号化データを第２復号化鍵にて復号化させて復号化データとするプログラム起動手段と、前記プログラム起動手段にて暗号化データの復号化が完了すると、復号化されて起動対象となった前記プログラムを消去するプログラム消去手段と、を備えたことを特徴とする復号化システムである。

【００１８】請求項１２記載の発明は、更に、前記暗号化データに含まれる暗号化された第２復号化鍵を、使用者に対応する復号化鍵にて復号化する鍵復号化手段を備えた請求項１１記載の復号化システムである。

【００１９】請求項１３記載の発明は、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、前記本体装置が、前記プログラム暗

号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段を備える請求項１１記載の復号化システムである。

【００２０】請求項１４記載の発明は、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム復号化手段、前記プログラム起動手段、および前記プログラム消去手段を備え、前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記鍵復号化手段を備える請求項１２記載の復号化システムである。

【００２１】請求項１５記載の発明は、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段および前記鍵復号化手段を備える請求項１２記載の復号化システムである。

【００２２】請求項１６記載の発明は、前記付属装置が、前記復号化鍵を直接記憶せず、前記復号化鍵が必要とされた場合に、対応する管理コードを用いた演算にて、前記復号化鍵を生成する請求項１３～１５のいずれかに記載の復号化システムである。

【００２３】請求項１７記載の発明は、前記プログラムが、所定時間以内に使用者により次の入力操作が行われない場合に、自己の処理を中止して、前記プログラム消去手段の処理を実行させる機能を有する請求項１１～１６記載の復号化システムである。

【００２４】請求項１８記載の発明は、請求項１～１０のいずれか記載の暗号化システムと請求項１１～１７記載の復号化システムとが組合わされてなる情報秘匿処理システムである。請求項１９記載の発明は、前記暗号化データを通信回線を介して相手方に送信する送信手段を備える請求項１～１０のいずれか記載の暗号化システムである。

【００２５】請求項２０記載の発明は、前記暗号化データを通信回線を介して受信する受信手段を備える請求項１１～１７のいずれか記載の復号化システムである。請求項２１記載の発明は、請求項１９記載の暗号化システムと請求項２０記載の復号化システムとが組合わされてなる情報秘匿通信システムである。

【００２６】

【作用及び発明の効果】請求項１の暗号化システムは、プログラム暗号化記憶手段、プログラム読出手段、プログラム復号化手段、プログラム起動手段およびプログラム消去手段を備え、プログラム暗号化記憶手段は、暗号化処理用のプログラムを、使用者に対応する第１暗号化鍵により暗号化した状態で記憶する。プログラム読出手段は、前記プログラム暗号化記憶手段内から、使用者に対応する第１暗号化鍵にて暗号化された前記プログラムを読み出す。プログラム復号化手段は、前記プログラム読出手段により読み出された前記プログラムを、使用者に対応する復号化鍵により復号化する。プログラム起動手段は、前記プログラム復号化手段により復号化されたプログラムを起動させることにより、暗号化対象データを第２暗号化鍵にて暗号化させて暗号化データとする。プログラム消去手段は、前記プログラム起動手段にて暗号化対象データの暗号化が完了すると、復号されて起動対象となった前記プログラムを消去する。

【００２７】このように、本発明の暗号化システムにて起動する暗号化処理用のプログラムは、暗号化処理に用いられていない場合には、プログラム暗号化記憶手段により暗号化された状態で記憶されている。したがって、暗号化されたままでは、第三者により、解析されることはなく、また解析できないので改竄もできない。また、復号化鍵は使用者が所持することにより、第三者にプログラム復号化手段が判明しても暗号化処理用のプログラムを復号化することはできない。

【００２８】正当な使用者がデータを暗号化する場合には、プログラム読出手段が、プログラム暗号化記憶手段内から、使用者に対応する第１暗号化鍵にて暗号化された前記プログラムを読み出し、プログラム復号化手段が、そのプログラムを、使用者に対応する復号化鍵により復号化し、プログラム起動手段が、その復号化されたプログラムを起動させる。この起動された前記プログラムの機能により、暗号化対象データが第２暗号化鍵にて暗号化されて暗号化データとなる。

【００２９】しかも、データの暗号化が完了した後は、プログラム消去手段が、その起動された平文状態のプログラムを消去する。このため、暗号化処理をした後も、平文状態の暗号化用のプログラムが残っていることがなく、暗号化用のプログラムの安全性が確保され、結果として、暗号化されたデータの安全性も確保される。したがって、暗号化処理毎に、暗号化処理用のプログラムを記憶している記憶媒体を保管場所から取り出してコンピュータにセットしてロードする作業をしなくても良く、効率的に暗号化作業ができる。

【００３０】上記構成に更に、鍵暗号化手段および鍵付加手段を加えても良い。この鍵暗号化手段は、前記第２暗号化鍵を、第３暗号化鍵にて暗号化する。そして、鍵付加手段は、前記鍵暗号化手段にて暗号化された前記第２暗号化鍵を、前記暗号化データに付加する。

【００３１】このように、データを暗号化するための第２暗号化鍵を、更に第３暗号化鍵にて暗号化しているの

で、鍵付加手段にて、暗号化データに第２暗号化鍵を付加しておいても安全は確保できる。また、暗号化データに第２暗号化鍵が付加されるので、その記憶媒体のまま持ち運んだり、あるいはその暗号化データを通信により相手方に送信しても、持ち運び先あるいは通信相手先にて、第３暗号化鍵さえ保管されていれば、暗号化データを復号化することができる。すなわち、暗号化データに付加されている暗号化された第２暗号化鍵を第３暗号化鍵にて復号化し、次に復号化された第２暗号化鍵にて、暗号化データを復号化することができる。尚、鍵付加手段は、前記暗号化用のプログラムの機能として実現されていても良い。

【００３２】更に、この場合、第２暗号化鍵が、前記暗号化用のプログラムにより演算にて求められたものであっても良い。このように演算にて求められる暗号化鍵は一時的な鍵であり、継続して使用されるものではないので、よりデータの安全性が確保される。また、この一時的な鍵も、上記暗号化用のプログラムにて演算されていることから、暗号化処理時以外は、その第２暗号化鍵を生成するプログラムは暗号化されたもののみが存在しているので、第三者が知っている鍵を生成するように改竄することはできない。

【００３３】また、本暗号化システムは、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とに別れて構成されていても良い。例えば、本体装置を、コンピュータ装置とし、付属装置を、ＩＣカードとする構成が挙げられる。

【００３４】この場合、本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段を備える構成としても良い。

【００３５】このように構成すると、暗号化処理をしない場合には、本体装置から付属装置を切り離して、安全な保管場所に収納しておくことができる。付属装置側には、使用者に対応する復号化鍵とプログラム復号化手段とが存在するため、その復号化鍵およびプログラム復号化手段のプログラムの安全性が共に確保され、データの安全性が一層確保される。

【００３６】また、同様に、本体装置と付属装置とに別々に構成された場合に、本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム復号化手段、前記プログラム起動手段、および前記プログラム消去手段を備え、付属装置が、前記第３暗号化鍵を記憶するとともに、前記鍵暗号化手段を備える構成としても良い。

【００３７】このように構成すると、付属装置側には、第３暗号化鍵と鍵暗号化手段とが存在するため、その第３暗号化鍵および鍵暗号化手段のプログラムの安全性が共に確保され、データの安全性が一層確保される。また、本体装置と付属装置とに別々に構成された場合に、上記両者を加味した構成、すなわち、本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、付属装置が、前記使用者に対応する復号化鍵および前記第３暗号化鍵を記憶するとともに、前記プログラム復号化手段および前記鍵暗号化手段を備える構成としても良い。

【００３８】このように構成すると、付属装置側には、使用者に対応する復号化鍵、第３暗号化鍵、プログラム復号化手段および鍵暗号化手段とが存在するため、その使用者に対応する復号化鍵、第３暗号化鍵、プログラム復号化手段のプログラムおよび鍵暗号化手段のプログラムの安全性がすべて確保され、データの安全性が一層確保される。

【００３９】また、前記付属装置が、第３暗号化鍵を、復号化を許可する者の管理コードと対応したリストとして記憶していても良い。このように構成されていると、管理コード、例えばＩＤにて復号化を許可する者を指定すれば、付属装置の鍵暗号化手段がそのＩＤに対応した第３暗号化鍵にて第２暗号化鍵を暗号化することができる。

【００４０】また、前記付属装置が、復号化鍵または第３暗号化鍵を直接記憶せず、復号化鍵または第３暗号化鍵が必要とされた場合に、対応する管理コードを用いた演算にて、復号化鍵または第３暗号化鍵を生成するものとしても良い。特に、第３暗号化鍵が多数記憶しなくてはならない場合に、演算式のみで良いのでメモリの節約となる。

【００４１】また前記プログラムが、所定時間以内に使用者により次の入力操作が行われない場合に、自己の処理を中止して、前記プログラム消去手段の処理を実行させる機能を有するものとしても良い。このようにすれば、正当な使用者がシステム装置から一旦離れたとしても、しばらくすると平文状態のプログラム自体が消え去るので第三者に解析されたり改竄されたりすることがない。

【００４２】請求項１１の復号化システムは、プログラム暗号化記憶手段、プログラム読出手段、プログラム復号化手段、プログラム起動手段およびプログラム消去手段とを備え、プログラム暗号化記憶手段は、前記プログラムを、使用者に対応する第１暗号化鍵により暗号化した状態で記憶し、プログラム読出手段は、前記プログラム暗号化記憶手段内から、使用者に対応する第１暗号化鍵にて暗号化された前記プログラムを読み出し、プログラム復号化手段は、前記プログラム読出手段により読み出された前記プログラムを、使用者に対応する復号化鍵により復号化し、プログラム起動手段は、前記プログラ

ム復号化手段により復号化された前記プログラムを起動させることにより、暗号化データを第２復号化鍵にて復号化させて復号化データとし、プログラム消去手段は、前記プログラム起動手段にて暗号化データの復号化が完了すると、復号化されて起動対象となった前記プログラムを消去する。

【００４３】このように、本発明の復号化システムにて起動する復号化処理用のプログラムは、復号化処理に用いられていない場合には、プログラム暗号化記憶手段により暗号化された状態で記憶されている。したがって、暗号化されたままでは、第三者により、解析されることはなく、また解析できないので改竄もできない。また、復号化鍵は使用者が所持することにより、第三者にプログラム復号化手段が判明しても復号化処理用のプログラムを復号化することはできない。

【００４４】正当な使用者が暗号化データを復号化する場合には、プログラム読出手段が、プログラム暗号化記憶手段内から、使用者に対応する第１暗号化鍵にて暗号化された前記プログラムを読み出し、プログラム復号化手段が、そのプログラムを、使用者に対応する復号化鍵により復号化し、プログラム起動手段が、その復号化されたプログラムを起動させる。この起動された前記プログラムの機能により、暗号化データを第２復号化鍵にて復号化させて復号化データ、すなわち平文データとすることができる。

【００４５】しかも、暗号化データの復号化が完了した後は、プログラム消去手段が、その起動された平文状態のプログラムを消去する。このため、復号化処理をした後も、平文状態の復号化用のプログラムが残っていることもなく、復号化用のプログラムの安全性が確保され、結果として、データの安全性も確保される。したがって、復号化処理毎に、復号化処理用のプログラムを記憶している記憶媒体を保管場所から取り出してコンピュータにセットしてロードする作業をしなくても良く、効率的に復号化作業ができる。

【００４６】上記構成に更に、鍵復号化手段をを加えても良い。この鍵復号化手段は、暗号化データに含まれる暗号化された第２復号化鍵を、使用者に対応する復号化鍵にて復号化する。このようにすることにより、暗号化データを復号化するための第２復号化鍵が得られ、正当な使用者のみが適切に暗号化データを復号化して平文データを得ることができる。

【００４７】また、本復号化システムは、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とに別れて構成されていても良い。例えば、本体装置を、コンピュータ装置とし、付属装置を、ＩＣカードとする構成が挙げられる。

【００４８】この場合、本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段を備える構成としても良い。

【００４９】このように構成すると、復号化処理をしない場合には、本体装置から付属装置を切り離して、安全な保管場所に収納しておくことができる。付属装置側には、使用者に対応する復号化鍵とプログラム復号化手段とが存在するため、その復号化鍵およびプログラム復号化手段のプログラムの安全性が共に確保され、データの安全性が一層確保される。

【００５０】また、同様に、本体装置と付属装置とに別々に構成された場合に、本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム復号化手段、前記プログラム起動手段、および前記プログラム消去手段を備え、付属装置が、使用者に対応する復号化鍵を記憶するとともに、前記鍵復号化手段を備える構成としても良い。

【００５１】このように構成すると、付属装置側には、使用者に対応する復号化鍵と鍵復号化手段とが存在するため、その復号化鍵および鍵復号化手段のプログラムの安全性が共に確保され、データの安全性が一層確保される。また、本体装置と付属装置とに別々に構成された場合に、上記両者を加味した構成、すなわち、本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段および前記鍵復号化手段を備える構成としても良い。

【００５２】このように構成すると、付属装置側には、使用者に対応する復号化鍵、プログラム復号化手段および鍵復号化手段とが存在するため、その使用者に対応する復号化鍵、プログラム復号化手段のプログラムおよび鍵復号化手段のプログラムの安全性がすべて確保され、データの安全性が一層確保される。

【００５３】また、前記付属装置が、復号化鍵を直接記憶せず、復号化鍵が必要とされた場合に、対応する管理コードを用いた演算にて、復号化鍵を生成するものとしても良い。また前記プログラムが、所定時間以内に使用者により次の入力操作が行われない場合に、自己の処理を中止して、前記プログラム消去手段の処理を実行させる機能を有するものとしても良い。このようにすれば、正当な使用者がシステム装置から一旦離れたとしても、しばらくすると平文状態のプログラム自体が消え去るので第三者に解析されたり改竄されたりすることがない。

【００５４】また、上述したいずれかの構成の暗号化システムと上述したいずれかの復号化システムとを組合わせて、情報秘匿処理システムとして構成しても良い。このことにより、一つの情報秘匿処理システムにて、暗号化システムと復号化システムとの両方の機能を有するこ

とができ、使用者の処理が効率的となるとともに、プログラムやデータの安全性も確保される。

【００５５】尚、上述した暗号化システムにおいて、暗号化データを通信回線を介して相手方に送信する送信手段を備えて、例えば暗号化機能を有するファクシミリ装置等のデータ通信システムとして構成することができる。また、上述した復号化システムにおいても同様に、暗号化データを通信回線を介して受信する受信手段を備えて、例えば暗号化データの解読機能を有するファクシミリ装置等のデータ通信システムとして構成することができる。

【００５６】勿論、上述の送信手段を有する暗号化システムと上述の受信手段を有する復号化システムとを組合わせ、暗号化機能および暗号化データ解読機能を有するファクシミリ装置等の情報秘匿通信システムとして構成することができる。

【００５７】

【実施例】図１および図２は、本発明の情報秘匿処理システムの一実施例を示している。この内、図１は、情報処理装置２のブロック図を示す。情報処理装置２は、ＣＰＵ４、ＲＯＭ６、ＲＡＭ８、バックアップＲＡＭ１０、キーボード１２、光磁気ディスク（ＭＯＤ）ドライブ１４、ＣＲＴディスプレイ１６、ハードディスク（ＨＤ）装置１８、フロッピーディスク（ＦＤ）ドライブ２０および入出力インターフェイス（Ｉ／Ｏ）２２を備えている。これらの構成はバス２４にて信号的に接続され、更にＩ／Ｏ２２にはＩＣカードリーダー２６が接続されている。

【００５８】このように、情報処理装置２はコンピュータとして構成され、ＲＯＭ６、光磁気ディスクドライブ１４に挿入された光磁気ディスク、ハードディスク装置１８、フロッピーディスクドライブ２０に挿入されたフロッピーディスクあるいはＩＣカードリーダー２６に挿入されたＩＣカード３０（図２）から読み込まれたプログラムやデータに基づいて、必要な処理を実行し、結果として得られたデータを、光磁気ディスクドライブ１４に挿入された光磁気ディスク、ハードディスク装置１８、フロッピーディスクドライブ２０に挿入されたフロッピーディスクあるいはＩＣカードリーダー２６に挿入されたＩＣカード３０に記憶する。情報処理装置２は、これ以外にＣＤ－ＲＯＭドライブ装置や磁気テープ記憶装置等を備えても良い。

【００５９】図２にＩＣカード３０のブロック図を示す。ＩＣカード３０は、ＣＰＵ３２、ＲＯＭ３４、ＲＡＭ３６、バックアップＲＡＭ３８および入出力インターフェイス（Ｉ／Ｏ）４０を備えている。これらの構成はバス４２にて信号的に接続されている。尚、Ｉ／Ｏ４０は、情報処理装置２のＩＣカードリーダー２６に対するコネクタを備えたインターフェイスである。

【００６０】前記情報処理装置２の電源オンにより、図３（ａ）に示すごとくＲＡＭ８のプログラムエリアに、データを暗号化および復号化するためのイニシャルプログラムＩＰがハードディスク装置１８からロードされて起動される。尚、ハードディスク装置１８には、図３（ｂ）に示すごとく、イニシャルプログラムＩＰ以外に、複数の暗号化された「第２の暗／復号化処理プログラム」Ｐｒ1～Ｐｒnが格納されている。これらの「第２の暗／復号化処理プログラム」Ｐｒ1～Ｐｒnは、本情報処理装置２の使用者の暗号化鍵（第１暗号化鍵）にて暗号化されたものであり、使用者の数だけ存在し、復号化すれば基本的には同じ機能を有しているプログラムである。ただし、後述するごとく使用者毎に異なる機能を持たせることもできる。使用者とプログラムとの対応は、図３（ｂ）に示すハードディスク装置１８内の使用者ＩＤ－プログラムアドレステーブルを参照することにより行われる。これらの「第２の暗／復号化処理プログラム」Ｐｒ1～Ｐｒnおよび使用者ＩＤ－プログラムアドレステーブルは、前記イニシャルプログラムＩＰとともにハードディスク装置１８に予めインストールされている。

【００６１】また、ＩＣカード３０のバックアップＲＡＭ３８には、図４に示すごとく、パスワード照合プログラムＰｒ11、暗号化処理プログラムＰｒ12、復号化処理プログラムＰｒ13、鍵暗号化処理プログラムＰｒ14および鍵復号化処理プログラムＰｒ15等のプログラムと、正当な使用者のパスワード、正当な使用者のＩＤ、正当な使用者の暗／復号化鍵（第１暗号化鍵および復号化鍵に該当する）および正当な使用者がデータの復号化を許可する相手のＩＤ（ＩＤ1，ＩＤ2，…，ＩＤn）とそのＩＤに対応する相手方暗号化鍵Ｋ1，Ｋ2，…，Ｋnが記憶されている。

【００６２】使用者が、データを暗号化するために、情報処理装置２を電源オンした場合には、図５および図６のフローチャートに示すイニシャルプログラムＩＰが起動される。まず、ステップＳ１００にて初期化処理が行われ、情報処理装置２に存在する各種構成の初期状態を設定し、プログラムに使用するデータの初期値を決定する等の処理がなされる。

【００６３】次に、ＩＣカードリーダー２６にＩＣカード３０が装着されているか否かが判定される（Ｓ１１０）。装着されていなければステップＳ１１０にては否定判定されて、ＩＣカード３０の装着を要求する表示をＣＲＴディスプレイ１６に行って（Ｓ１２０）、再度ステップＳ１１０を実行する処理を繰り返す。

【００６４】ＩＣカード３０が、ＩＣカードリーダー２６に装着されれば、ステップＳ１１０にて肯定判定されて、次にパスワードを要求する表示がＣＲＴディスプレイ１６になされる（Ｓ１３０）。このパスワードは、図４に示したＩＣカード３０の正当な使用者のパスワードを求めるものである。

【００６５】パスワードの入力がキーボード１２からな

されたか否かが判定され（Ｓ１４０）、入力が無ければ、ステップＳ１５０にてタイムアウトと判定されるまで、ステップＳ１４０，Ｓ１５０の処理を繰り返す。タイムアウトに該当する所定時間経過してもパスワードの入力がなされなければステップＳ１５０にて、肯定判定されて、本イニシャルプログラムの処理を終了する。タイムアウトする前にパスワードの入力があれば、ステップＳ１４０にて肯定判定されて、入力されたパスワードがＩＣカード３０側に送信される。そして、次に、ＩＣカード３０側からパスワードの照合結果とその使用者のＩＤとが送信されて来るのを待つ（Ｓ１７０）。

【００６６】図７～図８のフローチャートにＩＣカード３０側の処理を示す。本処理はＩＣカード３０がＩＣカードリーダー２６に装着された際に起動される処理である。まず、情報処理装置２からのパスワードの受信待ちとなる（Ｓ５００）。前述したステップＳ１６０の処理により、パスワードが送信されて来ればステップＳ５００にて肯定判定されて、パスワード照合プログラムＰｒ11により、図４に示したバックアップＲＡＭ３８に記憶された、このＩＣカード３０の正当な使用者のパスワードと、情報処理装置２から送られたパスワードとの照合がなされる（Ｓ５２０）。

【００６７】そして、その照合の結果と正当な使用者のＩＤとが情報処理装置２側へ送信される（Ｓ５３０）。次に照合結果が「合致」、すなわち、情報処理装置２からのパスワードとバックアップＲＡＭ３８内に記憶されていた正当使用者のパスワードとが一致すれば、正当な使用者がそのＩＣカード３０を使用していることが判るので、次にその正当な使用者の暗／復号化鍵を、バックアップＲＡＭ３８から読み出す（Ｓ５５０）。もし、パスワードの照合結果が不一致となった場合に、ステップＳ５４０にて否定判定されて、再度ステップＳ５００の処理に戻る。

【００６８】ステップＳ５５０を処理した場合には、次に情報処理装置２からの送信待ちとなる（Ｓ５６０）。ステップ５３０の処理にて、照合結果とＩＤとが情報処理装置２へ送信されると、情報処理装置２側では、ステップ１７０にて肯定判定されて、次に合致したか否かが判定される（Ｓ１８０）。合致していなければ、正当な使用者では無いので、ステップ１８０にて否定判定されて、ＣＲＴディスプレイ１６に、不一致であることと処理を中止するとの表示をして（Ｓ１９０）、ステップＳ１１０の処理に戻る。したがって、ＩＣカード３０がＩＣカードリーダー２６に装着されていれば、再度、ステップ１３０にてパスワードが要求され、ステップ１４０，Ｓ１５０にて、パスワード入力待ちとなる。パスワードの入力を間違えても、再度、入力を求められるので正当な使用者ならば訂正すれば良い。しかし、不正な使用である場合には、パスワードを繰り返して入力させるのは一致の可能性が高くなるので、パスワードの入力間違いは例えば３回までとし、ステップＳ１８０にて３回目の間違いの場合には、ステップＳ１１０に戻さず、本イニシャルプログラムを終了するようにする。

【００６９】ステップＳ１８０にて、合致したとの判定がなされると、ＣＲＴディスプレイ１６に合致した旨の表示がなされ（Ｓ２００）、次にＩＣカード３０から照合結果と共に受信したＩＤに対応する暗号化された第２の暗／復号化処理プログラムをハードディスク装置１８の記憶ファイルから探し出して、ＩＣカード３０側へ送信する（Ｓ２１０）。ＩＤからプログラムを探すのは、図３（ｂ）に示したごとく、ハードディスク装置１８にファイルされている使用者ＩＤ－プログラムアドレステーブルから、ＩＤに対応する暗号化された第２の暗／復号化処理プログラムのディスク上のアドレスを得て、そのアドレスから該当する暗号化された第２の暗／復号化処理プログラムを読み出すことにより行われる。例えば、使用者のＩＤがＩＤbであれば、暗号化された第２の暗／復号化処理プログラムＰr2が対応していることが、使用者ＩＤ－プログラムアドレステーブルから判明し、そのディスクアドレスから、暗号化された第２の暗／復号化処理プログラムＰr2が読み出される。

【００７０】次に、ＩＣカード３０からの送信待ちとなる（Ｓ２２０）。ＩＣカード３０側では、情報処理装置２から暗号化された第２の暗／復号化処理プログラムＰr2の送信があると、ステップＳ５６０の判定にて肯定判定されて、次にそのプログラムＰr2の受信とその受信したプログラムＰr2の復号化処理がなされる（Ｓ５７０）。すなわち、バックアップＲＡＭ３８に存在する復号化処理プログラムＰｒ13を起動して、情報処理装置２から送信されて来たプログラムＰr2を復号化する。尚、プログラムＰr2が長くて、バッファや作業メモリ容量の関係で一度に送信あるいは復号化できない場合には、分割して送信あるいは復号化しても良い。

【００７１】次に、復号化した第２の暗／復号化処理プログラムＰr2を情報処理装置２へ送信する（Ｓ５８０）。次に、暗号化していない一時鍵および復号化対象者ＩＤが受信されたか否かが判定され（Ｓ５９０）、受信していなければ、暗号化された一時鍵が受信されたか否かが判定される（Ｓ５９５）。これも受信していなければ、暗号化していない第２の暗／復号化処理プログラムが受信されたか否かが判定される（Ｓ６００）。いずれも受信していない内は、ステップＳ５９０，ステップＳ５９５およびステップＳ６００の判定を繰り返す。

【００７２】情報処理装置２側では、ＩＣカード３０側から、復号化された、すなわち平文の第２の暗／復号化処理プログラムＰr2を受信すると、ステップＳ２２０にて肯定判定されて、その平文の第２の暗／復号化処理プログラムＰr2を、図２（ａ）に示すごとくＲＡＭ８の作業メモリ領域ＰＡに転送する（Ｓ２３０）。

【００７３】次に、この平文の第２の暗／復号化処理プ

ログラムPr2がイニシャルプログラムから起動される（Ｓ２４０）。その第２の暗／復号化処理プログラムPr2のフローチャートを図９～図１２に示す。この処理がステップＳ２４０の起動処理により実行される。

【００７４】第２の暗／復号化処理プログラムPr2の処理が開始されると、まず、処理メニューがＣＲＴディスプレイ１６に表示される（Ｓ１０１０）。メニューは、暗号化処理（Ｓ１１００）、復号化処理（Ｓ１２００）、第２の暗／復号化処理プログラムの変更処理（Ｓ１３００）およびその他の処理（Ｓ１４００）である。

【００７５】ここで、使用者により暗号化処理（Ｓ１１００）が選択されると、図１０に示す処理が開始される。まず、暗号化対象データ名および復号化対象者ＩＤの入力が要求される（Ｓ１１０２）。暗号化対象データ名は、光磁気ディスクドライブ１４にセットされた光磁気ディスク、ハードディスク装置１８あるいはフロッピーディスクドライブ２０にセットされたフロッピーディスク内のファイルを指定することにより行う。ここでは、光磁気ディスクに暗号化データを格納するため、暗号化対象データは、フロッピーディスクに存在するものとする。

【００７６】また復号化対象者ＩＤは、復号化を許可する相手のＩＤを入力する。復号化を許可する相手方が複数であれば複数のＩＤを入力する。尚、予め登録されているグループのＩＤを入力すれば、そのグループに属している複数の相手のＩＤを指定したことになり、一つのＩＤで複数人を復号化対象者とすることができる。

【００７７】ここで、タイムアウト処理（Ｓ１１０６）にて所定のタイムアウト時間が経過するまで、入力待ちとなる（Ｓ１１０４）。タイムアウトまで、入力がなければ、ステップＳ１１０６にて肯定判定されて、直ちにイニシャルプログラムへ帰るが、暗号化対象データ名および復号化対象者ＩＤの入力がなされれば、次に一時鍵（第２暗号化鍵）を生成する（Ｓ１１０８）。

【００７８】ここで、一時鍵の生成は、生成毎に異なる鍵（値や文字列）であることが好ましい。例えば、Ｍ系列乱数発生プログラムによる方法やキー操作の時間間隔を１０万分の１秒程度で測定して下位の必要桁数のみ取り出す方法等が挙げられる。こうして生成された一時鍵と復号化対象者ＩＤとをＩＣカード３０側へ送信し（Ｓ１１１０）、次にＩＣカード３０側から送信されて来る暗号化された一時鍵の受信待ちとなる（Ｓ１１２０）。

【００７９】ＩＣカード３０側では、一時鍵と復号化対象者ＩＤとを受信したので、図８のステップＳ５９０にて肯定判定されて、次に、一時鍵暗号化処理プログラムＰｒ14により、復号化対象者ＩＤに対応する相手方暗号化鍵により一時鍵を暗号化する（Ｓ６１０）。ＩＣカード３０のバックアップＲＡＭ３８には、図４に示したごとく、正当な使用者がデータの復号化を許可する相手のＩＤ1，ＩＤ2，…，ＩＤnとそのＩＤに対応する相手方暗号化鍵K1，K2，…，Knが記憶されていることから、例えば、復号化対象者ＩＤがＩＤ2であれば、対応する相手方暗号化鍵K2が選択され、その相手方暗号化鍵K2により一時鍵を暗号化する。また、グループのＩＤが入力されていれば、そのグループの代表となる者のＩＤから相手方暗号化鍵を選択してその相手方暗号化鍵にて一時鍵を暗号化してもよく、またグループ独自の相手方暗号化鍵にて一時鍵を暗号化しても良い。

【００８０】次にこのように暗号化された一時鍵を情報処理装置２側へ送信し（Ｓ６２０）、ＩＣカード３０での処理はステップＳ５００の処理に戻る。情報処理装置２側では、暗号化された一時鍵を受信したので、ステップＳ１１２０にて肯定判定されて、暗号化された一時鍵を、ＩＤとともに記憶媒体にファイルとして格納する（Ｓ１１３０）。この記憶媒体は、使用者が指定する記憶媒体であるが、ここでは、光磁気ディスクドライブ１４にセットされた光磁気ディスクである。勿論、フロッピーディスクあるいはハードディスク装置１８その他の記憶媒体でも良い。

【００８１】次に既にステップＳ１１０２にて入力されている暗号化対象データが読み出され（Ｓ１１４０）、暗号化されていない一時鍵、すなわちステップＳ１１０８で生成されたままの一時鍵により、その暗号化対象データが暗号化される（Ｓ１１５０）。このようなデータを鍵を用いて暗号化処理するプログラムとしては、米国の標準アルゴリズムであるＤＥＳや、ＮＴＴ社が開発したＦＥＥＬ等が知られている。

【００８２】次に、この暗号化されたデータを、ＩＤおよび暗号化された一時鍵が格納されたファイルに格納する（Ｓ１１６０）。すなわち、図１３に示すごとく、ヘッダー部として、復号者（復号を許可する者）のＩＤ(1)，ＩＤ(2)，…，ＩＤ(n)とそのＩＤに対応した暗号化一時鍵Ｋ(1)，Ｋ(2)，…，Ｋ(n)とのリストを記載し、データ部として、一時鍵にて暗号化した暗号化データを記載したファイルとして格納する。

【００８３】こうして、情報処理装置２にて暗号化処理（Ｓ１１００）が終了し、次にＲＡＭ８上に、例えば、ステップＳ１１４０の処理にてＲＡＭ８の作業メモリ領域に読み出されたままの暗号化対象データといった、暗号化されていないデータが存在する場合には、そのデータをクリアする処理（Ｓ１５００）が行われる。

【００８４】こうして、第２の暗／復号化処理が終了し、イニシャルプログラムに戻る。イニシャルプログラムでは、図６に示すステップＳ２５０の処理が行われて、ＲＡＭ８上に存在している第２の暗／復号化処理プログラムをクリアし、ステップＳ１１０の処理に戻る。

【００８５】このようにして、データの暗号化が終了する。上述したごとく、本実施例の情報処理装置２にて起動する暗号化処理用のプログラム（図９，図１０）は、暗号化処理に用いられていない場合には、ハードディス

ク装置１８により暗号化された状態で記憶されている。したがって、第三者により、解析されることはなく、また解析できないので改竄もできない。

【００８６】正当な使用者がデータを暗号化する場合には、ハードディスク装置１８から、正当な使用者の暗／復号化鍵にて暗号化された前記プログラムを読み出し、そのプログラムを、正当な使用者の暗／復号化鍵により復号化し、その復号化されたプログラムを起動させることにより、暗号化対象データを一時鍵（第２暗号化鍵）にて暗号化させて暗号化データとすることができる。

【００８７】しかも、データの暗号化が完了した後は、その起動されたプログラムを消去する。このため、暗号化処理をした後も、平文状態の暗号化用のプログラムが残っていることもなく、暗号化用のプログラムの安全性が確保され、結果として、暗号化されたデータの安全性も確保される。したがって、暗号化処理毎に、暗号化処理用のプログラムを記憶している記憶媒体を保管場所から取り出して情報処理装置２にセットしてロードする作業をしなくても良く、効率的に暗号化作業ができる。

【００８８】また、暗号化前のデータも作業メモリ領域上に残っている場合には、それをクリアしているので、より安全性が高い。更に、一時鍵（第２暗号化鍵）は、相手方暗号化鍵（第３暗号化鍵）にて暗号化される。そして、この暗号化された一時鍵は復号化を許可する者のＩＤとともに、暗号化データと一つのファイルに収納される。

【００８９】このように、データを暗号化するための一時鍵（第２暗号化鍵）を、更に相手方暗号化鍵（第３暗号化鍵）にて暗号化しているので、暗号化データに一時鍵（第２暗号化鍵）を付加しておいても安全は確保できる。また、暗号化データに一時鍵（第２暗号化鍵）が付加されるので、その記憶媒体（ここでは光磁気ディスク）のまま持ち運んだり、あるいはその暗号化データを通信により相手方に送信しても、持ち運び先あるいは通信相手先にて、相手方暗号化鍵（第３暗号化鍵）さえ保管されていれば、暗号化データを復号化することができる。

【００９０】一時鍵（第２暗号化鍵）は、前記暗号化用のプログラムにより演算にて求められたものである。このようにデータを暗号化するための暗号化鍵は、その時の暗号化のためだけの一時的な鍵であり、継続して使用されるものではないので、よりデータの安全性が確保される。また、この一時鍵も、前記暗号化用のプログラム内で演算されていることから、暗号化処理時以外は、そのプログラムは暗号化されたもののみが存在しているので、第三者は自分が知っている鍵を生成するように改竄することはできない。

【００９１】また、本実施例の情報秘匿処理システムは、本体装置としての情報処理装置２と、この情報処理装置２とは別体に構成され情報処理装置２に対して信号的に任意に接続したり切断したりすることが可能な付属装置としてのＩＣカード３０とに別れて構成され、しかも、情報処理装置２が、プログラム暗号化記憶処理、プログラム読出処理、プログラム起動処理、およびプログラム消去処理の各プログラムを備え、ＩＣカード３０が、正当な使用者の暗／復号化鍵および相手方暗号化鍵（第３暗号化鍵）を記憶するとともに、プログラム復号化処理および鍵暗号化処理の各プログラムを備える構成とされている。すなわち、ＩＣカード３０側には、正当な使用者の暗／復号化鍵、相手方暗号化鍵（第３暗号化鍵）、プログラム復号化処理のプログラムおよび鍵暗号化処理のプログラムが存在するため、その正当な使用者の暗／復号化鍵、相手方暗号化鍵（第３暗号化鍵）、プログラム復号化処理のプログラムおよび鍵暗号化処理のプログラムの安全性が確保され、データの安全性が一層確保される。

【００９２】次に、図１３に示した暗号化データファイルを格納した光磁気ディスクを受け取った場合、そのデータを復号化する処理について説明する。使用者は、まず、情報処理装置２の電源オンさせた後、受け取った光磁気ディスクを光磁気ディスクドライブ１４にセットし、自己のＩＣカード３０をＩＣカードリーダー２６にセットする。

【００９３】情報処理装置２では、イニシャルプログラムが起動される。この場合の処理は、ステップＳ１００からステップＳ２４０までは、データ暗号化の際に説明した通りである。ＩＣカード３０においても同様である。勿論、使用者が異なれば、ＩＣカード３０も異なることから、ステップＳ１７０にて受信するＩＤも異なり、ステップＳ２１０にてＩＣカード３０へ送信される暗号化された第２の暗／復号化処理プログラムも異なる。

【００９４】例えば、使用者のＩＤがＩＤaであれば、暗号化された第２の暗／復号化処理プログラムPr1が対応していることから、暗号化された第２の暗／復号化処理プログラムPr1が、ＩＣカード３０へ送信され、その結果、ステップＳ２４０により起動されるプログラムは、第２の暗／復号化処理プログラムPr1が実行される。尚、ここでは、第２の暗／復号化処理プログラムPr1は第２の暗／復号化処理プログラムPr2と同じ内容であるとして説明する。

【００９５】ステップＳ２４０にて第２の暗／復号化処理プログラムPr1が起動されると、まず、図９に示すフローチャートのステップＳ１０１０にて、処理メニューの表示がなされる。ここで使用者が復号化処理を選択すると、ステップＳ１２００の処理が開始される。この復号化処理を図１１のフローチャートに示す。

【００９６】まず、復号化対象データ名入力の要求が表示される（Ｓ１２０２）。次にステップＳ１２０６にてタイムアウトと判定されるまでその入力待ち（Ｓ１２０

4）となる。入力がなされずにタイムアウトとなればステップＳ１２０６にて肯定判定されて、第２の暗／復号化処理を終了し、イニシャルプログラムに帰る。

【００９７】光磁気ディスクドライブ１４にセットされた光磁気ディスク内の一つのデータファイルを指定した場合（光磁気ディスク内のファイルすべてを指定しても良いし、特定のディレクトリ内のファイルをすべて指定しても良い。）、ステップＳ１２０４にて肯定判定されて、その復号化対象の暗号化データのヘッダー部より復号化対象者ＩＤ(1)，ＩＤ(2)，…および対応する暗号化された一時鍵Ｋ(1)，Ｋ(2)，…を読み出す（Ｓ１２０８）。

【００９８】次にこの復号化対象者ＩＤ(1)，ＩＤ(2)，…内に、使用者のＩＤが存在するか否かが判定される（Ｓ１２１０）。すなわち、ＩＣカードリーダー２６にセットされているＩＣカード３０に記載されている使用者のＩＤが、復号化対象者として指定されているか否かが判定される。存在しなければ、現在セットされているＩＣカード３０の正当な使用者は、復号化は許可されていないので、ステップＳ１２１０にて否定判定されて、復号化は不許可であることをＣＲＴディスプレイ１６に表示して（Ｓ１２２０）、第２の暗／復号化処理を終了して、イニシャルプログラムに戻る。尚、複数のファイルが復号化対象として指示された場合には、ＩＣカード３０に記載されている使用者のＩＤが復号化対象者としてヘッダー部に指定されているファイルが一つでも存在すれば、その含まれているファイルについてだけステップＳ１２３０以降の処理を行う。また、ヘッダー部にグループのＩＤが指定されている場合には、ＩＣカード３０の正当使用者がそのグループに含まれていれば、その正当使用者はヘッダー部に指定されているとする。

【００９９】ＩＣカード３０に記載された正当な使用者のＩＤが、復号化対象者ＩＤ(1)，ＩＤ(2)，…内に含まれている場合、例えば、ＩＤ(1)が該当すると、ステップＳ１２１０にて肯定判定されて、復号化対象ファイルのヘッダー部から読み出した暗号化された一時鍵Ｋ(1)を、ＩＣカード３０側へ送信し（Ｓ１２３０）、次に復号化された一時鍵の受信待ち（Ｓ１２４０）となる。

【０１００】ＩＣカード３０側にて、ステップＳ５９０，Ｓ５９５およびＳ６００を繰り返している状態で、暗号化された一時鍵Ｋ(1)を受信すると、ステップＳ５９５にて肯定判定されて、一時鍵復号化処理プログラムＰｒ15により、暗号化された一時鍵Ｋ(1)を、バックアップＲＡＭ３８に記憶している正当な使用者の暗／復号化鍵で復号化する（Ｓ６３０）。

【０１０１】次に復号化された一時鍵を情報処理装置２へ送信し（Ｓ６４０）、ステップＳ５００の処理に戻る。情報処理装置２側では、復号化された一時鍵を受信したので、ステップＳ１２４０にて肯定判定されて、復号化対象データのデータ部を復号化された一時鍵で復号化して記憶媒体に格納する（Ｓ１２５０）。

【０１０２】こうして復号化処理（Ｓ１２００）が終了すると、前述したステップＳ１５００にて、ＲＡＭ８上に暗号化されていないデータ、すなわち復号化されたデータが存在する場合には、そのデータをクリアする処理が行われる。こうして、第２の暗／復号化処理が終了し、イニシャルプログラムに戻る。イニシャルプログラムでは、図６に示すステップＳ２５０の処理が行われて、ＲＡＭ８上に存在している第２の暗／復号化処理プログラムをクリアし、ステップＳ１１０の処理に戻る。

【０１０３】このようにして、データの復号化が終了する。上述したごとく、本実施例の情報処理装置２にて起動する復号化処理用のプログラム（図９，図１１）は、復号化処理に用いられていない場合には、ハードディスク装置１８により暗号化された状態で記憶されている。したがって、第三者により、解析されることはなく、また解析できないので改竄もできない。

【０１０４】正当な使用者が復号化データを復号化する場合には、ハードディスク装置１８から、正当な使用者の暗／復号化鍵にて暗号化された前記プログラムを読み出し、そのプログラムを、正当な使用者の暗／復号化鍵により復号化し、その復号化されたプログラムを起動させることにより、暗号化データを一時鍵（第２復号化鍵に該当する。すなわち一時鍵は第２暗号化鍵でも有り、第２復号化鍵でもある。）にて復号化させて復号化データ、すなわち平文データとすることができる。

【０１０５】しかも、暗号化データの復号化が完了した後は、その起動されたプログラムを消去する。このため、復号化処理をした後も、平文状態の復号化用のプログラムが残っていることもなく、復号化用のプログラムの安全性が確保され、結果として、データの安全性も確保される。したがって、復号化処理毎に、復号化処理用のプログラムを記憶している記憶媒体を保管場所から取り出して情報処理装置２にセットしてロードする作業をしなくても良く、効率的に復号化作業ができる。

【０１０６】また、復号化されたデータも作業メモリ領域上に残っている場合には、それをクリアしているので、より安全性が高い。更に、暗号化データに含まれる暗号化された一時鍵（第２復号化鍵）を、正当な使用者の暗／復号化鍵にて復号化する。

【０１０７】このようにすることにより、暗号化データを復号化するための一時鍵（第２復号化鍵）が得られ、正当な使用者のみが適切に暗号化データを復号化して平文データを得ることができる。また、本実施例では、本体装置としての情報処理装置２と、この情報処理装置２とは別体に構成され情報処理装置２に対して信号的に任意に接続したり切断したりすることが可能な付属装置としてのＩＣカード３０とに別れて構成され、情報処理装置２が、プログラム暗号化記憶処理、プログラム読出処理、プログラム起動処理、およびプログラム消去処理の

各プログラムを備え、ＩＣカード３０が、正当な使用者の暗／復号化鍵を記憶するとともに、プログラム復号化処理および鍵復号化処理のプログラムを備える構成とされている。

【０１０８】このように構成されているため、ＩＣカード３０側には、正当な使用者の暗／復号化鍵、プログラム復号化処理および鍵復号化処理のプログラムが存在するため、その正当な使用者に対応する暗／復号化鍵、プログラム復号化処理のプログラムおよび鍵復号化処理のプログラムの安全性が確保され、データの安全性が一層確保される。

【０１０９】次に、ハードディスク装置１８に記憶されている、暗号化された第２の暗復号化処理プログラムの変更処理について説明する。使用者は、まず、情報処理装置２の電源オンさせた後、受け取った光磁気ディスクを光磁気ディスクドライブ１４にセットし、自己のＩＣカード３０をＩＣカードリーダー２６にセットする。

【０１１０】情報処理装置２では、イニシャルプログラムが起動される。この場合の処理は、ステップＳ１００からステップＳ２４０までは、データ暗号化あるいは復号化の際に説明した通りである。ＩＣカード３０においても同様である。勿論、使用者が異なれば、ＩＣカード３０も異なることから、ステップＳ１７０にて受信するＩＤも異なり、ステップＳ２１０にてＩＣカード３０へ送信される暗号化された第２の暗／復号化処理プログラムも異なる。

【０１１１】例えば、使用者のＩＤがＩＤcであれば、暗号化された第２の暗／復号化処理プログラムPr3が対応していることから、暗号化された第２の暗／復号化処理プログラムPr3が、ＩＣカード３０へ送信され、その結果、ステップＳ２４０により起動されるプログラムは、第２の暗／復号化処理プログラムPr3が実行される。　ステップＳ２４０にて第２の暗／復号化処理プログラムPr3が起動されると、まず、図９に示すフローチャートのステップＳ１０１０にて、処理メニューの表示がなされる。

【０１１２】ここで使用者がプログラム変更処理を選択すると、ステップＳ１３００の処理が開始される。プログラム変更処理を図１２のフローチャートに示す。まず、第２の暗／復号化処理プログラムの編集処理がなされる（Ｓ１３０２）。例えば、１６進数にて表現されている第２の暗／復号化処理プログラムを逆アセンブルして、アセンブリ言語にて表現し、キーボード１２による編集可能とする。編集が終了すれば、編集後の内容がアセンブルされ、実行可能なプログラムに変換される。

【０１１３】尚、この編集処理では、単に既に変更されている他のプログラムと置き換える処理も含まれる。したがって、他の装置で作成したプログラムを新たに、第２の暗／復号化処理プログラムとして取り込むことができる。また、この編集処理では、単にプログラム中に設定されている数値や文字列等のデータの変更も含まれる。

【０１１４】次に、編集後の第２の暗／復号化処理プログラムをＩＣカード３０側へ送信し（Ｓ１３０４）、暗号化された第２の暗／復号化処理プログラムの受信待ち（Ｓ１３０６）となる。ＩＣカード３０側にて、ステップＳ５９０，Ｓ５９５およびＳ６００を繰り返している状態で、暗号化していない第２の暗／復号化処理プログラムを受信すると、ステップＳ６００にて肯定判定されて、プログラム暗号化処理プログラムＰｒ12により、ＩＣカード３０の正当な使用者の暗／復号化鍵により第２の暗／復号化処理プログラムを暗号化する（Ｓ６５０）。

【０１１５】次に、この暗号化された第２の暗／復号化処理プログラムを情報処理装置２へ送信し（Ｓ６６０）、ステップＳ５００の処理に戻る。情報処理装置２側では、暗号化された第２の暗／復号化処理プログラムを受信したので、ステップＳ１３０６にて肯定判定され、次に暗号化された第２の暗／復号化処理プログラムをハードディスク装置１８に収納し、そのディスクアドレスを、使用者ＩＤ－プログラムアドレステーブルの内、ＩＤcと対応させたプログラムアドレスＰｒ3に記入する（Ｓ１３０８）。

【０１１６】こうして、プログラム変更処理を終了する。以後、ステップＳ１５００の処理を行って、イニシャルプログラムに帰る。イニシャルプログラムでは、ステップＳ２５０の処理が行われて、ＲＡＭ８上に存在している第２の暗／復号化処理プログラムをクリアし、ステップＳ１１０の処理に戻る。

【０１１７】上述したごとく、本実施例の情報処理装置２にて起動するプログラム変更処理（図９，図１２）は、正当な使用者により、その使用者専用の暗号化された第２の暗／復号化処理プログラムの内容を変更できるので、その使用者毎に異なるアルゴリズムや異なる設定値（プログラム中のデータを変更した場合）にて暗／復号化することが可能となる。

【０１１８】したがって、使用者毎にプログラムを変更しておけば、一人の暗／復号化アルゴリズムが第三者に解析された場合にも、同時に全員のプログラムまで解析されることはない。また、解析された場合には、プログラム変更処理により、正当な使用者がプログラムを変更することにより、以後の情報については安全性が確保できる。

【０１１９】また本実施例において、入力操作が行われない場合は、タイムアウト処理（Ｓ１１０６，Ｓ１２０６）により第２の暗／復号化処理プログラムを終了し、ステップＳ２５０のの処理が行われて、ＲＡＭ８上に存在している第２の暗／復号化処理プログラムをクリアしているので、使用者が処理の途中で情報処理装置２を離れても、第三者による解析や改竄を防止できる。ステッ

プS１３０２にても編集の途中で操作が行われなくなれば、第２の暗／復号化処理プログラムを終了しても良い。

【０１２０】また、情報処理装置２側では、データ量の大きい暗号化対象のデータの暗号化あるいは復号化処理を行い、ＩＣカード３０側では、データ量の小さいプログラムや一時鍵の暗号化あるいは復号化処理を行うので、全体の処理としては高速に行うことができる。また、ＩＣカード３０としては小さくて安価な構成とすることができる。

【０１２１】また、図１３に示したごとく、復号化を許可する者の数に対応して暗号化されるのは一時鍵のみであり、実際の暗号化データは一つのみ存在することから、保管、運搬あるいは通信するデータ量は、復号化を許可する者の数が多くても、膨大なデー多量とはならず、メモリや記憶媒体あるいは通信時間が節約できる。

【０１２２】本実施例において、ハードディスク装置１８がプログラム暗号化記憶手段に該当し、ステップＳ２１０がプログラム読出手段としての処理に該当し、ステップＳ５７０がプログラム復号化手段としての処理に該当し、ステップＳ２４０がプログラム起動手段としての処理に該当し、ステップＳ２５０がプログラム消去手段としての処理に該当し、ステップＳ６１０が鍵暗号化手段としての処理に該当し、ステップＳ１１６０が鍵付加手段としての処理に該当し、ステップＳ６３０が鍵復号化手段としての処理に該当する。

【０１２３】［その他］上述した実施例は、データを暗号化したり、あるいは暗号化したデータを復号化して平文データに戻す情報秘匿処理システムであったが、更に、情報処理装置２が網制御装置およびモデムを備えることにより、正当な使用者が前記実施例のごとくデータを暗号化して通信回線を介して相手方に送信し、また相手方が通信回線を介して送信して来た暗号化データを、前記実施例のごとく正当な使用者（復号化対象者）が復号化して平文データとして得る情報秘匿通信システムとして構成しても良い。

【０１２４】更に、この情報秘匿通信システムに、原稿の画像読取装置および画像の記録装置を備えることにより、ファクシミリ装置として構成し、その原稿の画像データを、前記実施例のごとく、暗号化あるいは復号化の対象としても良い。前記実施例では、正当使用者や復号化対象者をＩＤで指定していたが、ＩＤでなくても対象者名でも良いし、ＩＤと対象者名との両方でも良い。

【０１２５】前記実施例では、ＩＣカード３０に記憶されている正当使用者の暗／復号化鍵は、暗号化にも復号化にも用いられたが、暗号化時は公開鍵を用い、復号化時には秘密鍵を用いても良い。したがって、正当な使用者がデータの復号化を許可する相手方暗号化鍵Ｋ1，Ｋ2，…，Ｋnは公開鍵であっても良い。

【０１２６】またＩＣカード３０のバックアップＲＡＭ３８には、復号化を許可する相手方のＩＤ1，ＩＤ2，…とそれに対応した暗号化鍵Ｋ1，Ｋ2，…とが記憶されていたが、直接、このようなＩＤと暗号化鍵Ｋとを記憶するのではなく、次のようにしても良い。

【０１２７】すなわち、バックアップＲＡＭ３８に秘密のアルゴリズムを内蔵し、復号化を許可する相手方のＩＤを入力すると、そのアルゴリズムにしたがって演算処理にて対応する暗号化鍵Ｋを生成する構成としても良い。この構成にすると複数の暗号化鍵を記憶しなくても、一つのアルゴリズムのみで、多数のＩＤから暗号化鍵を得ることができるので、復号化を許可する者が多い場合には、メモリの節約となる。

【０１２８】このＩＤから演算処理で鍵を生成する構成を、ＩＣカード３０の正当な使用者の暗／復号化鍵に対しても適用して、正当な使用者のＩＤから暗／復号化鍵を生成するようにしても良い。また、ＩＣカード３０は、バックアップＲＡＭ３８にプログラムや各鍵等を保管しているので、外装に連動して外装開放時にオフとなるスイッチをバックアップ電源とバックアップＲＡＭ３８との間に用いれば、外装を開けるとプログラムや鍵等が消去されることから、安全上、より好ましい。また、バックアップＲＡＭ３８の代りに、ＥＥＰＲＯＭにプログラムや鍵等を記憶しても良い。この場合は、外装と連動して外装開放時にオンとなるスイッチを電源とＥＥＰＲＯＭとの間に設ければ、外装を開けると電流が流れてプログラムや鍵等が消去される。

【０１２９】前記実施例において、イニシャルプログラムはハードディスク装置１８でなく、ＲＯＭ６に格納されていても良い。

【図面の簡単な説明】

【図１】　本発明一実施例を構成する情報処理装置のブロック図である。

【図２】　本発明一実施例を構成するＩＣカードのブロック図である。

【図３】　情報処理装置におけるプログラムおよびデータの記憶配置説明図である。

【図４】　ＩＣカードにおけるプログラムおよびデータの記憶配置説明図である。

【図５】　情報処理装置におけるイニシャルプログラムのフローチャートである。

【図６】　情報処理装置におけるイニシャルプログラムのフローチャートである。

【図７】　ＩＣカード側処理のフローチャートである。

【図８】　ＩＣカード側処理のフローチャートである。

【図９】　第２の暗／復号化処理のフローチャートである。

【図１０】　第２の暗／復号化処理の内の暗号化処理のフローチャートである。

【図１１】　第２の暗／復号化処理の内の復号化処理のフローチャートである。

【図１２】 第２の暗／復号化処理の内のプログラム変更処理のフローチャートである。

【図１３】 暗号化データの構成説明図である。

【符号の説明】

２…情報処理装置　４…ＣＰＵ　６…ＲＯＭ　８…ＲＡＭ

１０…バックアップＲＡＭ　１２…キーボード

１４…光磁気ディスクドライブ　１６…ＣＲＴディスプレイ

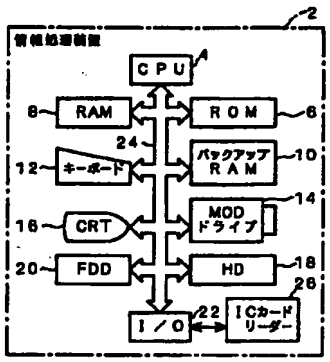
１８…ハードディスク装置　２０…フロッピーディスクドライブ

２２…Ｉ／Ｏ　２４…バス　２６…ＩＣカードリーダー

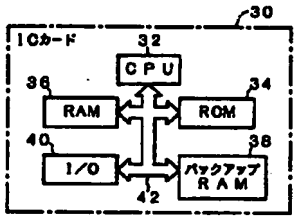
３０…ＩＣカード　３２…ＣＰＵ　３４…ＲＯＭ　３６…ＲＡＭ

３８…バックアップＲＡＭ　４０…Ｉ／Ｏ　４２…バス

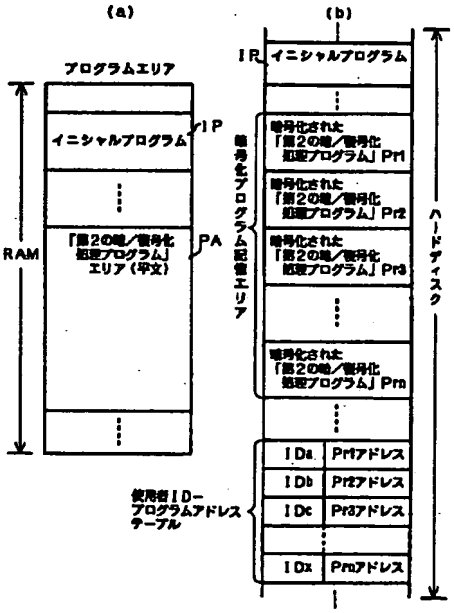
【図１】



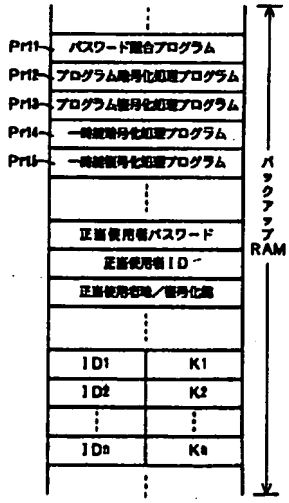
【図２】



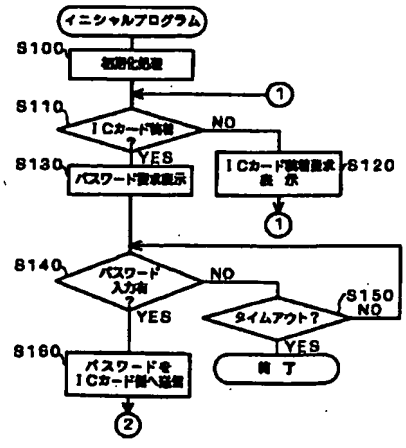
【図３】



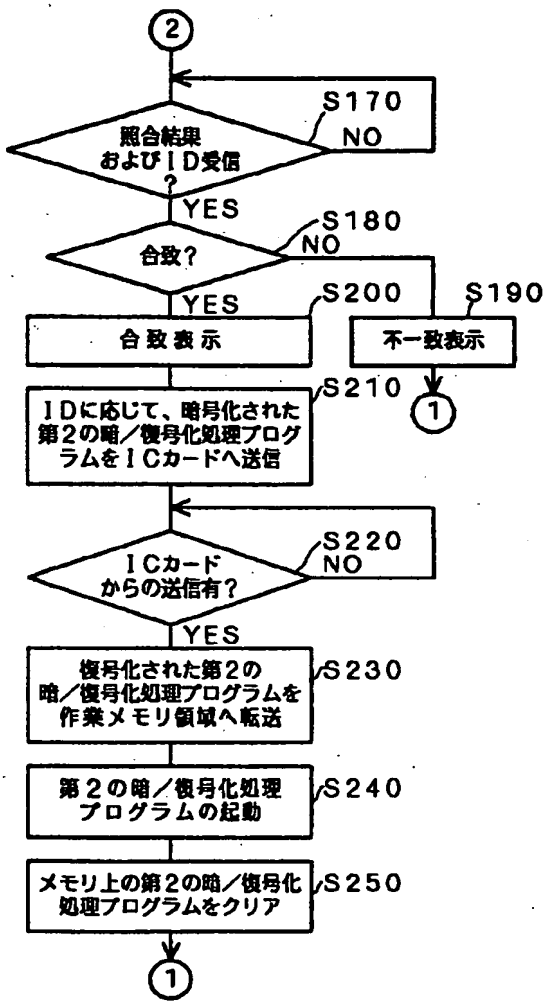
【図４】



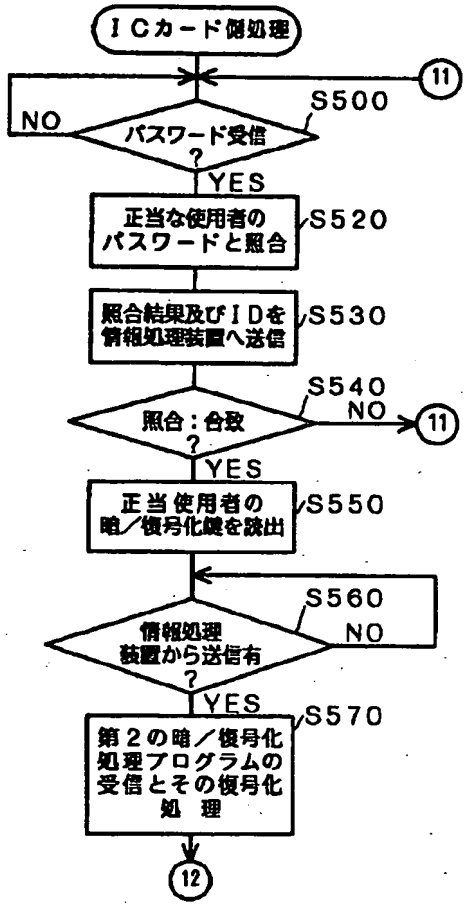
【図５】



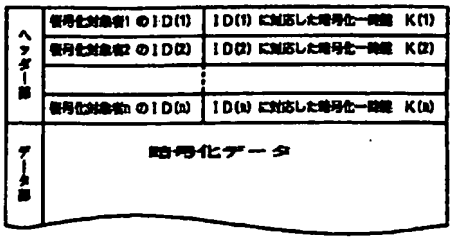
【図6】


②
S170
照合結果およびＩＤ受信？
NO
YES
S180
合致？
NO
YES
S200
合致表示
S190
不一致表示
①
S210
ＩＤに応じて、暗号化された第２の暗／復号化処理プログラムをＩＣカードへ送信
S220
ＩＣカードからの送信有？
NO
YES
S230
復号化された第２の暗／復号化処理プログラムを作業メモリ領域へ転送
S240
第２の暗／復号化処理プログラムの起動
S250
メモリ上の第２の暗／復号化処理プログラムをクリア
①

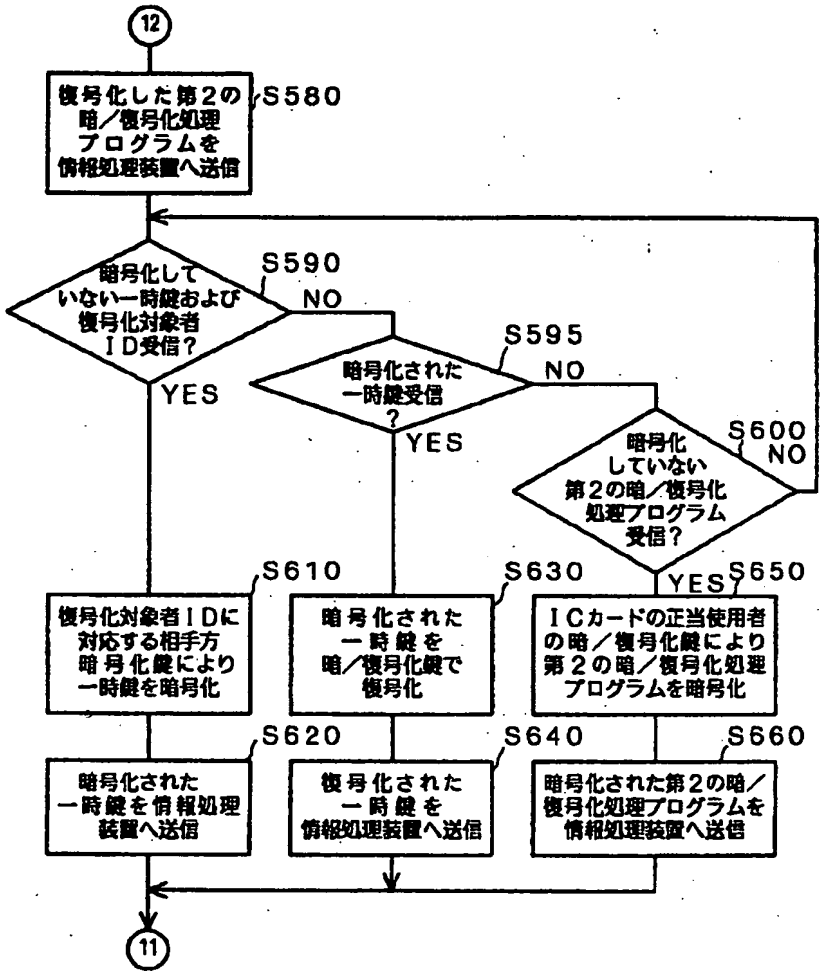
【図7】


ＩＣカード側処理
⑪
S500
NO
パスワード受信？
YES
S520
正当な使用者のパスワードと照合
S530
照合結果及びＩＤを情報処理装置へ送信
S540
照合：合致？
NO
⑪
YES
S550
正当使用者の暗／復号化鍵を読出
S560
情報処理装置から送信有？
NO
YES
S570
第２の暗／復号化処理プログラムの受信とその復号化処理
⑫

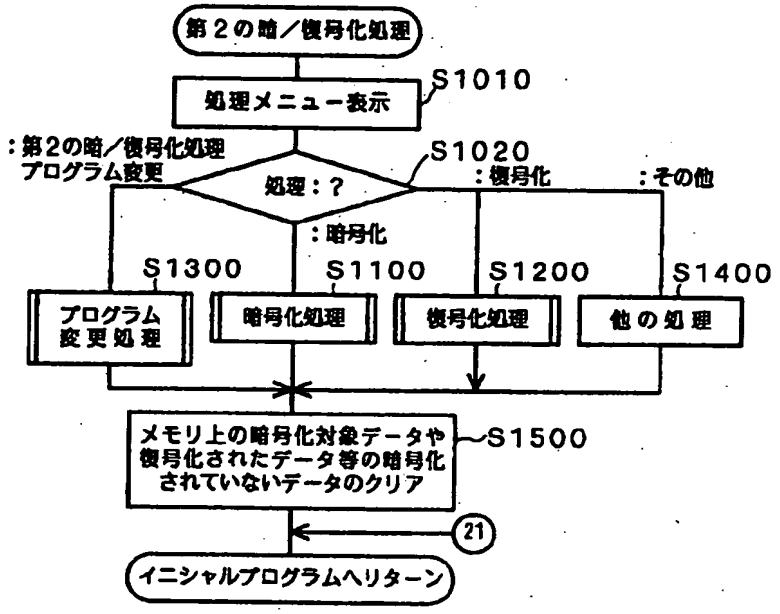
【図13】


ヘッダー部
ＩＤ(1)
ＩＤ(2)
ＩＤ(n)
データ部
暗号化データ

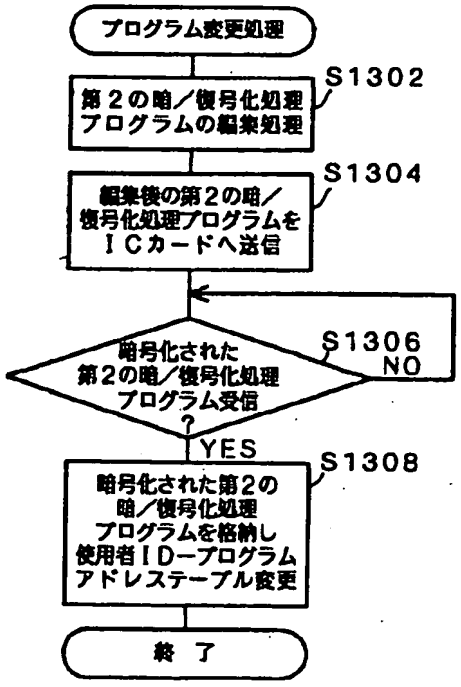
【図8】


12
復号化した第2の暗／復号化処理プログラムを情報処理装置へ送信
S580
暗号化していない一時鍵および復号化対象者ＩＤ受信？
S590
NO
YES
暗号化された一時鍵受信？
S595
NO
YES
暗号化していない第2の暗／復号化処理プログラム受信？
S600
NO
YES
復号化対象者ＩＤに対応する相手方暗号化鍵により一時鍵を暗号化
S610
暗号化された一時鍵を暗／復号化鍵で復号化
S630
ＩＣカードの正当使用者の暗／復号化鍵により第２の暗／復号化処理プログラムを暗号化
S650
暗号化された一時鍵を情報処理装置へ送信
S620
復号化された一時鍵を情報処理装置へ送信
S640
暗号化された第２の暗／復号化処理プログラムを情報処理装置へ送信
S660
11

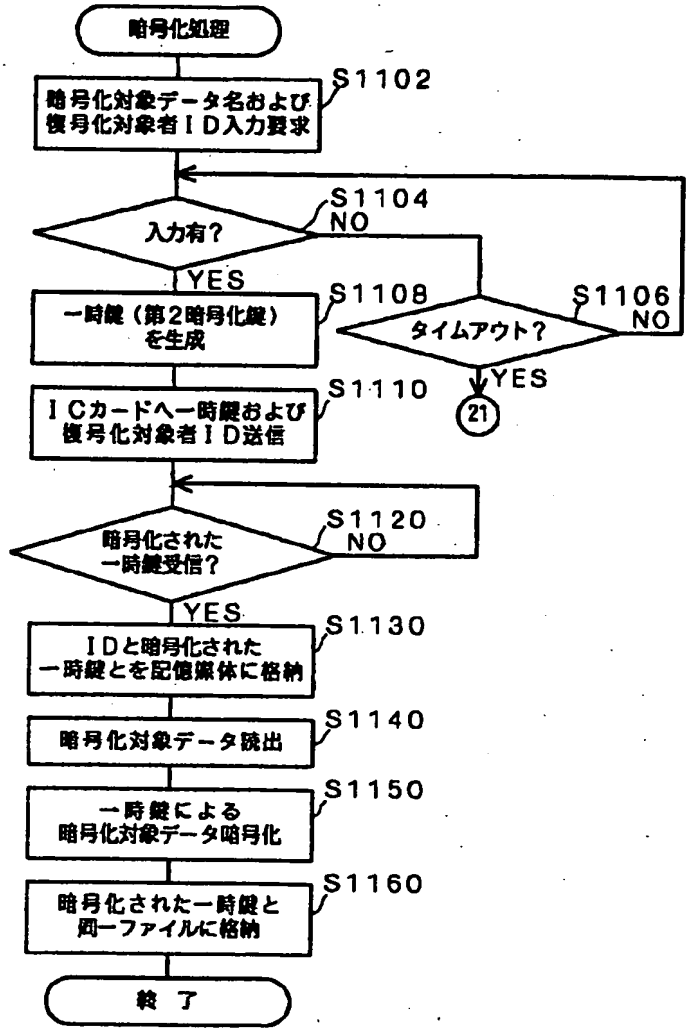
【図9】


第２の暗／復号化処理
処理メニュー表示
S1010
：第２の暗／復号化処理プログラム変更
処理：？
S1020
：暗号化
：復号化
：その他
S1300
S1100
S1200
S1400
プログラム変更処理
暗号化処理
復号化処理
他の処理
メモリ上の暗号化対象データや復号化されたデータ等の暗号化されていないデータのクリア
S1500
21
イニシャルプログラムへリターン

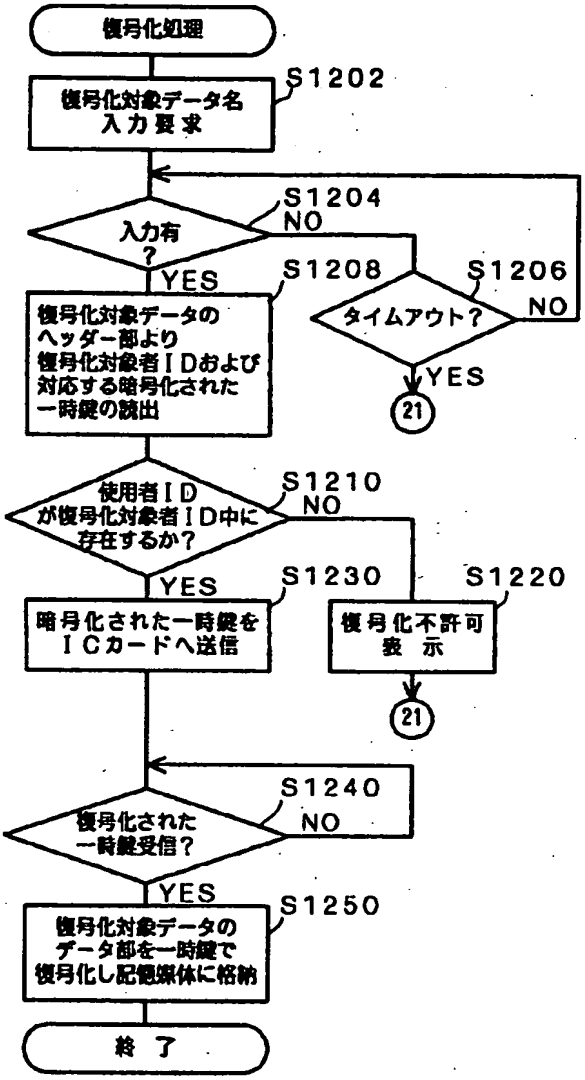
【図１２】


プログラム変更処理
第２の暗／復号化処理プログラムの編集処理
S1302
編集後の第２の暗／復号化処理プログラムをＩＣカードへ送信
S1304
暗号化された第２の暗／復号化処理プログラム受信？
S1306
NO
YES
暗号化された第２の暗／復号化処理プログラムを格納し使用者ＩＤ－プログラムアドレステーブル変更
S1308
終了

【図１０】


暗号化処理
S1102
暗号化対象データ名および
復号化対象者ＩＤ入力要求
S1104
NO
入力有？
YES
S1108
一時鍵（第２暗号化鍵）
を生成
S1106
NO
タイムアウト？
YES
21
S1110
ＩＣカードへ一時鍵および
復号化対象者ＩＤ送信
S1120
NO
暗号化された
一時鍵受信？
YES
S1130
ＩＤと暗号化された
一時鍵とを記憶媒体に格納
S1140
暗号化対象データ読出
S1150
一時鍵による
暗号化対象データ暗号化
S1160
暗号化された一時鍵と
同一ファイルに格納
終 了

【図１１】


復号化処理
S1202
復号化対象データ名
入力要求
S1204
入力有
？
NO
YES
S1208
復号化対象データの
ヘッダー部より
復号化対象者ＩＤおよび
対応する暗号化された
一時鍵の読出
S1206
タイムアウト？
NO
YES
21
S1210
使用者ＩＤ
が復号化対象者ＩＤ中に
存在するか？
NO
YES
S1230
暗号化された一時鍵を
ＩＣカードへ送信
S1220
復号化不許可
表示
21
S1240
復号化された
一時鍵受信？
NO
YES
S1250
復号化対象データの
データ部を一時鍵で
復号化し記憶媒体に格納
終了

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.